aruba
a Hewlett Packard
Enterprise company

Remote Access Points: Network Beyond the Corporate Campus

By Kevin Blackburn, Blog Contributor

When it comes to enterprise networking, designing and maintaining a corporate campus has a unique set of challenges. Adding in a remote workforce makes this challenge even bigger. Modern remote workforces now include users at small remote offices and even users working from home. Normally, providing wireless network access on campus is straightforward but takes a lot of the time: Set up a controller, conduct a site survey and deploy access points to cover the needed areas. The problem is that area you need to cover just got bigger!

Bringing the Network to Remote Locations

When it comes to remote locations, the problem is that you might want to put in a full array of hardware, but for a small amount of users it just isn't worth it. So what do you do? You might drop in some standalone access points for wireless access. Do this for multiple locations and you have a management nightmare on your hands.

About the Author

Kevin Blackburn
Blog Contributor

Kevin blogs at The Routing Table, a networking and technology blog focusing on networking, certification and technical development.

With Aruba Remote Access Points (RAP), you can use the wireless controller that is already available at your main campus and allow the access points from these remote locations to associate, via the web, through a secure IPSec tunnel. Provisioning, authentication and configuration all can be managed from your controller. This is a large advantage over standalone access points at remote locations. This allows you to start treating your remote locations just like you would the main campus.

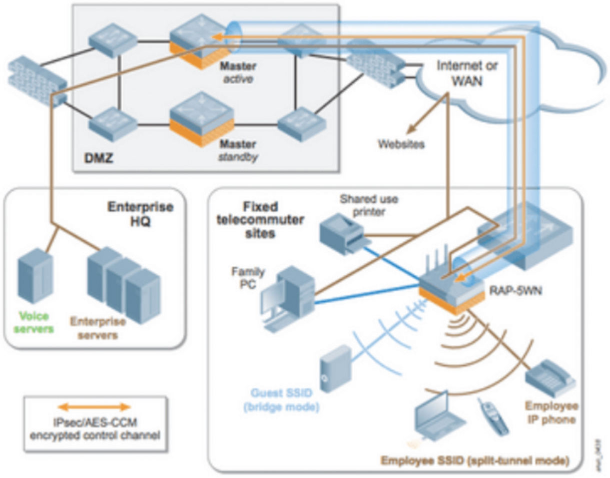

Figure 23 ***Remote employee network***

Photo Credit: Aruba RAP Deployment Guide

Configuring a RAP

Set up of your RAP is a very simple process once the controller is configured to support them. First, the new access point needs to be authorized to be used as a RAP. Authorizing a new RAP is quickly done with the new device's MAC address by adding it to the controller at the main campus.

The AP group is specified at this time as well. This will include many of the settings it will receive as well as the specific deployed WLANs. Next, via a wired connection to the new access point, the remote access point provisioning console is launched when a browser is opened on a connected laptop, for instance. Finally, you point the access point to the IP or host name of your controller.

From here, the device downloads any needed updates and configuration per the AP group policy it was assigned. After the information is received, the device will reboot and begin operating as a remote access point. Deploying access points in this manner means the engineers are no longer required to be the ones to travel to these remote locations to be the one to control the deployment.

More than Just Wireless

Giving users access to the corporate wireless network at remote locations or even their home is a very useful and beneficial feature, but there is one more thing that I really like. Aside from providing wireless network access with RAPs, you can also allow a wired device to be connected and have its connection tunneled back to the corporate campus. Very valuable for things like networked printers or any other wired devices. Dot1x is even a supported option for additional security.

The fact is that remote access points are a very cost effective way to extend your corporate network to smaller locations that normally would not justify the cost of the equipment to stand up a dedicated network topology. Now with nothing more than a basic network connection and an Aruba RAP, users can remain connected when away from the office, while maintaining the security that is required in enterprise networks.

Follow Kevin Blackburn on Twitter at @TheRoutingTable.